Enterprise Information Security Policies

State of Tennessee
Department of Finance and Administration
Office for Information Resources
Information Security Program

Document Version 1.6 – April 4, 2008

Table of Contents

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the availability, integrity and confidentiality of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been developed to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.

- Any computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.

- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

This document applies to all full- and part-time employees of the State of Tennessee and all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency IT professionals and approval by the Chief Information Security Officer (CISO) and executive management team within the Office for Information Resources, Department of Finance and Administration.

All information resources and any information system owned by the State of Tennessee shall be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the state government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee as well as the General Information Security Policy of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes cutting out existing processes which could introduce delays, or bypassing process requirements all together to keep up with the demand of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need and put the information security programs to work. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policy is a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 17799 standard framework. The policies are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

Scope (2.1)
The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, personal digital assistants (PDAs) and mobile devices (computing platforms) controlled by the State of Tennessee where lawfully permitted.

- Any computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.

- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

All full- and part-time employees of the State of Tennessee and all third parties, contractors, or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms shall adhere to the policies and requirements set forth in this document.

Authority (2.2)
The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Office for Information Resources (OIR) to establish and enforce policy and statewide standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. The Office for Information Resources is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

Reference:

Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994
ISC Information Resource Policies, Policy 1.00
ISC Information Resource Policies, Policy 13.00

Exceptions (2.3)
All exceptions to any of the security policies shall be reviewed by the Security Advisory Council (SAC) and approved by the Chief Information Security Officer. The exception request process and form can be found in the appendix of this document.

Review (2.4)
Review of this document takes place within the Security Advisory Council sessions and will occur on a semi-annual basis at a minimum. Document review can also be requested by sending a request to the OIR Security Management Team.

The official policy document and supporting documentation will be published on the OIR intranet site located at:

http://intranet.state.tn.us/finance/oir/security/policy.html

Document Format (2.5)
This document generally follows the International Standards Organization (ISO) 17799 standard framework for information technology security management. Each section starts with a high-level policy statement for the domain that is discussed in that section. The high-level policy statement is followed by the objectives of the section. More detailed or specific policy statements follow the objectives. The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise. Finally, the section closes with a description of responsibilities for the Office for Information Resources, agencies and individuals.

X. Section Name

High-level policy statement for section

OBJECTIVES:

Policy Name(x.x)

Policy statement.

Sub-Policy Name(x.x.x)

Sub-policy statement.

Policy Name(x.x)

Policy statement.

Policy Maintenance (2.6)
All policies will be maintained in accordance with the OIR policy process documentation. See the Security Policy Development and Implementation Process located in the appendix of this document.

3. GENERAL INFORMATION SECURITY POLICY

All information resources and information systems owned by the State of Tennessee shall be protected from unauthorized disclosure, use, modification or destruction in a manner consistent with their value, sensitivity and criticality to the business and operation of the state government and those it serves. The State of Tennessee shall institute an information security program to define the overall information security policy and direction.

OBJECTIVES:

- Ensure that the State of Tennessee's information resources are adequately and appropriately protected against unavailability, unauthorized access, modification, destruction or disclosure as required by the Information Systems Council of the State of Tennessee.
- Ensure that the State of Tennessee provisions an information security program to uphold the State of Tennessee's information security requirements.
- Ensure that authorized access to the State of Tennessee's information resources is appropriately provisioned.
- Prevent disruption of business processes or service delivery caused by information security inadequacies.
- Ensure that the information security posture of the State of Tennessee is appropriately, efficiently and effectively communicated to the stakeholders of the State of Tennessee.
- Define and assign responsibilities for protecting information technology resources.

RESPONSIBILITIES:

OIR

OIR is responsible for establishing and maintaining a statewide information security policy and security program. OIR will ensure that any information processing system attached to the State of Tennessee's enterprise network and managed by OIR, or on behalf of OIR, is compliant with this policy document. OIR will ensure that this policy document and any subsequent additions, changes or deletions are communicated appropriately to all agencies of State government.

Agency

Agencies are responsible for ensuring that any information processing system attached to the State of Tennessee's enterprise network and managed by the agency, or on behalf of the agency, is compliant with this policy document. Agencies are responsible for developing and implementing procedures and operations processes that support the goals and objectives of this policy document. Agencies may develop agency-specific policy documents provided the minimum requirements set forth in this document are met. Agencies are responsible for communicating this policy document throughout the agency.

Users

Users are responsible for adhering to statewide and agency policies, standards, procedures and guidelines pertaining to information security.

4. ORGANIZATIONAL SECURITY POLICY

The State of Tennessee shall maintain an organization within the Office for Information Resources (OIR) that is directly responsible for the direction and strategy of the information security program within the State of Tennessee and for all agencies of Tennessee state government. This group shall be led by the Chief Information Security Officer (CISO) who is ultimately responsible for the direction of the program and for reporting on the State's security posture to the Chief Information Officer (CIO) of the State of Tennessee. Each state agency shall appoint an information security "point of contact" (POC).

OBJECTIVES:

- Ensure that the State of Tennessee provisions an information security organization, led by a Chief Information Security Officer, to support the State of Tennessee's information security requirements.
- Ensure that the information security program can adequately address the requirements set forth by the Information Systems Council.
- Ensure that the State of Tennessee provisions an information Security Incident Response Team with appropriate resources to exercise the State of Tennessee's information security incident response plan when appropriate.
- Ensure that agencies designate a knowledgeable information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding information security within the agency.

Information Security Infrastructure (4.1)

OIR Security Management shall initiate and control an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

Incident Response Policy (4.2)

The State of Tennessee shall establish an information Security Incident Response Team (SIRT). The SIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The SIRT members will be appointed based on their position and capabilities within the organization. Each agency shall designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC shall have responsibility for incident escalations, actions and authority for the administrative oversight of security for the information technology resources under the agency's control. The POC within each agency will

participate as a member of the SIRT. The CISO of the State of Tennessee will appoint members from within OIR to participate in the SIRT.

Incident Response Plan (4.3)

See the appendix of this document.

RESPONSIBILITIES:

OIR

OIR is responsible for the establishment of the information security organization as well as the appointment of a Chief Information Security Officer (CISO). The CISO is responsible for the fostering, leadership and communication of the State of Tennessee's enterprise security program. The CISO shall establish a Security Advisory Council (SAC). As Chair of the Security Advisory Council (SAC), the CISO will ensure that the proper representatives are appointed to the SAC and will lead the SAC's efforts to develop, implement and maintain an information security program for the State of Tennessee. The CISO will chair the SIRT and ensure that it will be appropriately staffed and provisioned, organized, maintained, and will include a representative from each agency. The CISO will also ensure that an information security response plan is developed, maintained, and distributed to all agencies.

Agency

Agencies are responsible for appointing an information security POC. In accordance with ISC policies, the agency POC will have the responsibility and authority for the administrative oversight of security for information resources under the agency's control. The POC shall be available to work with the SIRT and knowledgeable of the information incident response plan. Further, agencies will ensure that the agency POC participates in the "Tennessee Agency Security Advisory Group" chaired by the CISO.

Users

Users are responsible for reporting suspected or known security violations to the agency's POC and for following instructions pertaining to specific incidents as provided by SIRT members.

5. ASSET CLASSIFICATION AND CONTROL POLICY

All information resource assets owned by the State of Tennessee shall be classified in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification or destruction. Classified assets shall be protected in a manner consistent with their value, sensitivity and criticality to the business and operation of the state government and those it serves or as specified by any superseding State or Federal law or regulation.

Accountability of Assets (5.1)

All information resource assets owned by the State of Tennessee shall be accounted for and have a designated custodian. Custodians shall be identified for all information resource assets by each State agency, and the responsibility for the maintenance of appropriate controls, or stewardship, shall be assigned for the assets under the agency's control. Accountability shall remain with the designated custodian of the asset.

Data Classification (5.2)

Data stored or transferred by information resource assets owned by the State of Tennessee shall be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable State and/or Federal law and regulations to indicate the need, priorities and degree of protection it will receive. At a minimum data shall be classified as public or confidential.

Public Data Classification Control (5.2.1)

Data classified as public shall be protected from unauthorized modification or destruction.

Confidential Data Classification Control (5.2.2)

Data classified as confidential shall be protected from unauthorized disclosure, use, modification or destruction.

RESPONSIBILITIES:

OIR

OIR is responsible for the development and maintenance of the statewide information resources asset classification requirements. OIR shall identify asset custodians for the information resources under their direct control. OIR asset custodians shall classify the assets under their control at the time the assets are assigned or created. Asset classification and maintenance can be delegated to an asset steward supervised by the asset custodian.

Agency

Agencies are responsible for identifying asset custodians for the resources under their direct control. Agency asset custodians shall classify the assets under their direct control at the time the assets are assigned or created. Asset classification and maintenance can be delegated to an asset steward supervised by the asset custodian.

Users

Users shall responsibly work with the assets they are assigned and due care shall be taken to protect any mobile computing asset from theft or destruction. Users shall not provide access to information resource assets without obtaining authorization from the asset custodian.

6. PERSONNEL SECURITY POLICY

Personnel Background Investigation (6.1)

Under Development

Acceptable Use Policy (6.2)

See the appendix of this document.

7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Physical access to the State of Tennessee's information resource assets and infrastructure will be restricted to individuals who require that access to perform their job function.

OBJECTIVES:

- To prevent unauthorized access, damage or interference to State of Tennessee premises and information.
- To prevent loss, damage or compromise of processing equipment or network components.

Secure Areas (7.1)

Critical/sensitive business information processing facilities shall be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls that protect them from unauthorized access, damage and/or interference.

Physical Security Perimeter (7.1.1)

All critical/sensitive enterprise processing facilities shall have multiple layers of physical security. Each layer shall be independent and separate of the preceding and/or following layer(s).

All other processing facilities shall have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Equipment Security (7.2)

Processing equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and to reduce the opportunities for unauthorized access.

Equipment Placement and Protection (7.2.1)

Equipment shall be located in secured areas. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter shall be locked in a secured cabinet with access controlled by the State of Tennessee. Secured cabinets or facilities shall support further segregation within the State of Tennessee's Information Technology (IT) organization based on role and responsibility.

Power Supplies (7.2.2)

Infrastructure and related computing equipment shall be protected from power failures and other electrical anomalies.

Cabling Security (7.2.3)

Power and telecommunications cabling carrying data or supporting information services shall be protected from unauthorized interception or damage.

General Security Controls (7.3)

Information shall be protected from disclosure to, modification or theft by unauthorized persons.

Clear Screen Policy (7.3.1)

All endpoints that provide access to Information Processing Systems shall be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system shall automatically be implemented if the system has been left unattended.

All computing platforms with attached displays shall be oriented away from direct line of sight from unauthorized viewers.

RESPONSIBILITIES

OIR

OIR is responsible for developing requirements and guidelines for physical access to enterprise information resource assets and infrastructure. OIR will ensure that appropriate protective mechanisms are installed to restrict access to the enterprise information resource assets and infrastructure, in coordination with appropriate departments. Further, OIR will ensure physical access to enterprise assets is monitored, and unauthorized access is reported to management or the proper authorities.

Agency

Agencies are responsible for implementing practices and procedures and installing protective mechanisms to ensure local information assets are protected from unauthorized access. Agencies are also responsible for ensuring that physical access to agency hosted assets is monitored and that unauthorized access is reported to management or the proper authorities.

Users

Users should report any suspicious activity or persons to management or the proper authorities. Users should also refrain from behaviors that could compromise the physical protection of information technology resources such as willful assistance without proper identification, tailgating through doors or sharing facility access keys or codes.

8. COMMUNICATIONS AND OPERATIONS MANAGEMENT POLICY

All agencies of the State of Tennessee shall document and maintain standard security operating procedures and configurations for their respective operating environments.

OBJECTIVES:

- Reduce the risk of liability for the unauthorized usage of unlicensed software and minimize the threat of exposure due to software weaknesses and/or configurations.
- Prevent the automated propagation of malicious code and contamination of sterile environments attached to the enterprise network.
- Ensure that media resources containing sensitive data are sanitized before transferal or reuse and that they are destroyed when decommissioned and not selected for reuse or transfer.
- Protect critical state information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction.

Operational Procedures and Responsibilities (8.1)

The operating procedures identified by the security policy shall be documented and maintained by the appropriate process owners.

Documentation of Operating Procedures (8.1.1)

Operating procedures relating to security shall be treated as formal documents and changes shall be authorized by management.

Operational Change Control (8.1.2)

Changes to information processing facilities and systems shall be controlled and monitored for security compliance. Formal management responsibilities and procedures shall exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of the State of Tennessee's operational environment.

All written documentation generated by the change control policies shall be retained as evidence of compliance.

Segmentation and Layered Security (8.1.3)

The State of Tennessee's operational environment shall support segmentation and layered security technologies and configurations based on role, risk, sensitivity and access control rules.

Segregation of Duties (8.1.4)
Separation of Development and Production Facilities (8.1.5)
Production Environment Access Control (8.1.6)
Under Development

System Planning and Acceptance (8.2)

System Acceptance (8.2.1)

Under Development

Capacity Planning (8.3)

Under Development

Software Control (8.4)

All software installed within the State's operational environment shall support security mechanisms that provide data integrity, confidentiality and availability. Software shall support security event monitoring and audit ability.

Authorized and Licensed Software (8.4.1)

Only licensed software procured through State of Tennessee contracts or software acquired with Office for Information Resources (OIR) involvement in the procurement process shall be installed in the State's environment. Software that does not require a purchase (i.e. General Public License, FreeWare, ShareWare) shall be approved as a State standard software product through the State's architecture standards approval process.

Malicious Software Control (8.4.2)

All computing platforms that are attached to the State's enterprise technology infrastructure shall be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses and/or logic bombs.

Compromised System Policy (8.4.2.1)

Any system found infected with "Rootkit" malicious software is considered fully compromised. Fully compromised systems shall be removed from the operational environment. OIR Security Management reserves the right to seize any compromised system for forensic analysis.

Patch Management Control (8.4.3)

All applications and processing devices that are attached to the State's enterprise technology infrastructure shall be kept up to date with security related patches made available by the software or hardware vendor.

Media Handling and Security (8.4.4)

Software licensed to the State of Tennessee shall be installed only on systems or devices covered by the license agreement.

Application Control (8.4.5)

Under Development

Media Disposal and Reuse (8.5)

All data storage devices (media) subject to transfer or reuse must be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding State or Federal requirements. Media assets that are not subject to transfer or reuse must be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding State or Federal requirements.

RESPONSIBILITIES:

OIR

OIR is responsible for maintaining network infrastructure and enterprise component software and operating system configurations with the latest release of security related updates compatible with the State's enterprise environment and will provide a means by which authentic, tested and approved security related software updates can be deployed and implemented by agencies across the enterprise. OIR will deploy and monitor security control devices to facilitate a means by which all processing devices attached to the enterprise network environment can be protected from intentional or unintentional exposure to malicious software. OIR will establish, maintain, and follow procedures to prevent the propagation of malicious code and/or system abuse. OIR will develop and maintain supporting guidelines and documentation and will ensure that contracts for standard software products and media destruction services are maintained. Finally, OIR will work with vendors/contractors (engaged through OIR) and who are responsible for non-state managed devices to ensure they understand and comply with these responsibilities.

Agency

Agencies will establish agency policy and procedures for media disposal or reuse, including personally and/or contractor owned devices, and will ensure that any agency media disposal and reuse procedure complies with superseding State or Federal sanitizing requirements that may be specific for the agency. Agencies systems attached to the State of Tennessee's enterprise network will participate in enterprise patch management and malicious software control programs. Agencies will be responsible for testing patches prior to release in the agency's environment. Agencies will also ensure that all systems not able to participate in an automatic security related update process are kept up to date through an additional manual process. This process, along with the participating systems, must be documented and made available for periodic audit by the OIR Security Management Team. Agencies will utilize software products that have been approved as standard for the State of Tennessee. Finally, agencies will ensure vendors/contractors (engaged through the agency) who are responsible for non-state-managed devices understand and comply with these responsibilities.

Users

Users are responsible for ensuring that devices assigned to them retain the ability to participate in automatic security software update environments (i.e. Disabling automatic enterprise configurations is prohibited). Users are to only utilize software products that have been approved as standard for the State of Tennessee, and they are to abstain from downloading unauthorized software or installing personally owned software.

9. ACCESS CONTROL POLICY

Access to the State of Tennessee's information resources shall be granted consistent with the concept of least privilege. All information processing systems owned by the State of Tennessee shall have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use. All information processing systems shall have the capability to interact with the statewide access control environment. Access to any State of Tennessee information processing system is generally forbidden unless explicitly permitted.

OBJECTIVES:

- Ensure that authorized access to the State of Tennessee's information resources is appropriately provisioned.
- Ensure that unauthorized access to information resources is appropriately prevented.
- Minimize information technology risks through the use of access control methodologies and techniques.
- Ensure that a means to segment and control enterprise network traffic is implemented.
- Ensure that all interconnectivity between the State of Tennessee's enterprise network and any other network is provisioned securely.

Access Control Rules (9.1)

Access control rules and requirements to access the State of Tennessee's information resources shall be developed, documented and maintained by their respective resource owners. All agency specific-access control rules and requirements must be made available for audit by the Office for Information Resources (OIR) Security Management Team and in compliance with the State of Tennessee enterprise security policies. All enterprise access control rules and requirements must be approved by the OIR Security Management Team.

User Access Management (9.2)

All State of Tennessee agencies shall develop, document and maintain user access and account management procedures. These procedures shall include, but are not limited to, new account provisioning, account transfer and/or job profile changes and account termination and/or de-provisioning.

User Registration and Authorization (9.2.1)
Loss of User Privilege (9.2.1.1)
User Privilege Control (9.2.2)
Under Development

User Identification and Authorization (9.2.3)

At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

User Account Lockout (9.2.4)

Limits shall be set for the number of unsuccessful logins that can be attempted for a UserID.

User Password Management (9.2.5)

Passwords assigned to users must be created and managed to protect against unauthorized discovery or usage and must meet the minimum password requirements.

Review of User Access Rights (9.2.6)

Under Development

Network Access Control (9.3)

The State of Tennessee's enterprise network shall be designed to provide the ability to segregate and control traffic between systems, connected devices and third party environments based on role, risk and sensitivity. The enterprise network will allow for specific services at all seven layers of the Open Systems Interconnection (OSI) model to be made available or filtered, depending on legitimate business need. All access and connectivity to the State of Tennessee's enterprise network must comply with the State of Tennessee's security requirements for enterprise network interconnectivity. All access and connectivity to the State of Tennessee's enterprise network shall be granted consistent with the concept of least privilege. Access and connectivity to the State of Tennessee's enterprise network is generally forbidden unless explicitly permitted.

User Authentication for Network Connections (9.3.1)

Under Development

Segregation in Networks (9.3.2)

All enterprise network architectures operated by, or on behalf of, the State of Tennessee shall be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones shall be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the OIR Security Management Team.

Enterprise Interconnectivity Requirements (9.3.3)

All systems attached to the State of Tennessee's enterprise network shall comply with the security requirements for enterprise interconnectivity documentation.

Operating System Access Control (9.4)

Session Time Outs (9.4.1)

Password Management System (9.4.2)

Use of Shared Technology Resources (9.4.3)

Under Development

Logon Banner (9.4.4)

All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user logs in.

Mobile and Workstation Computing (9.5)

All mobile and workstation computing platforms, including but not limited to desktops, laptops, hand-held devices, and portable storage media, shall be protected from unauthorized use, modification or destruction. Mobile and workstation computing platform capabilities shall be granted to individuals or entities that require such access and facilities to perform their specific job related duties. Confidential data assets shall not be stored on mobile and/or workstation computing platforms unless absolutely necessary.

Mobile Computing Policy (9.5.1)

Mobile computing platforms shall be physically protected against theft when left unattended. Mobile computing platforms shall not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a mobile computing platform must have approval from the asset custodian for such storage. Confidential data assets which have been authorized for mobile use must be encrypted while stored on mobile computing platforms.

Workstation Computing Policy (9.5.2)

Workstation computing platforms shall be physically protected against theft when left unattended. Workstation computing platforms shall not store confidential data assets where it is not absolutely necessary to perform the specific job related duties. Storage of confidential data assets on a workstation computing platform must have approval from the asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation must be encrypted while stored on the workstation computing platform.

Monitoring System Access and Use (9.6)

Event Logging (9.6.1)

Clock Synchronization (9.6.2)

Under Development

RESPONSIBILITIES:

OIR

OIR will ensure that all enterprise networks are provisioned and segmented with the appropriate levels of security in regards to role, risk and sensitivity. They will also develop, implement and maintain guidelines for password management and maintenance. OIR will ensure that all third parties are aware of and compliant with the State of Tennessee's Third Party Connectivity Agreement prior to the establishment of the interconnection. OIR is responsible for the management and processing of granting or rejecting third party interconnectivity requests. OIR shall ensure that due diligence and care is taken to fulfill any protection requirements of the mobile computing platforms for which OIR is responsible.

Agency

Agencies are responsible for implementing a process for identifying and documenting legitimate "need" for users to have access to the State of Tennessee's information resources. This process will include review and revalidation of existing users. Agencies will ensure that all requirements of a third party network connection to the State of Tennessee's enterprise network are presented to the OIR Security Management Team for review, approval or rejection prior to implementing the connection. Agencies shall ensure that due diligence and care is taken to fulfill any protection requirements of the mobile computing platforms for which each agency is responsible.

Users

Individual users are uniquely identified by their respective access credentials and are responsible for maintaining the confidentiality of those credentials. Users should refrain from using authentication credentials intended for the protection of State of Tennessee assets on personal computing platforms or non-State related websites.

10. SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY

Systems Development and Maintenance Control Policy 10.0

Under Development

11. COMPLIANCE POLICY

All State of Tennessee agencies must be compliant with this security policy document

Compliance with Legal Requirements (11.1)

All State of Tennessee agencies must be compliant with any State or Federal regulatory requirements which supersede this policy document.

Applicable Legislation (11.1.1)

All State of Tennessee agencies must be compliant with any legislation enacted by the State of Tennessee in regards to the management of information resources on behalf of the State.

Data Protection and Privacy (11.1.2)

All State of Tennessee agency data custodians must ensure that all "Personal Information" data assets, as defined by applicable State and/or Federal law and regulations, are protected from unauthorized use, modification or disclosure.

Data Breach and Disclosure (11.1.3)

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties shall provide notice of the disclosure in accordance with TCA 47-18-2107(3)(A).

Internal Compliance Matrix (11.2)

See the Appendix of this document for the policy compliance matrix, which indicates the dates by which all agencies must be compliant with the relative policy components. Those agencies that can not meet the compliance deadline must file for an exception using the security policy exception process.

12. BUSINESS CONTINUITY MANAGEMENT POLICY

While Business Continuity Management is included in the International Standards Organization (ISO) 17799 standards, it is outside the scope of the security organization within OIR. Agencies are expected to collaborate with the State's administrative services agencies to ensure their ability to recover from any disaster and to maintain business operations.

13. VERSION HISTORY

Version 1.0 – May 10, 2006	*Initial draft review to agencies and SAC.*
Version 1.1 – June 27, 2006	*Fixed errors before official release.*
Version 1.2 – July 12, 2006	*Added policies 5.0, 5.1, 5.3, 5.3.1, 9.5, 9.5.1, 11.1, 11.1.1, 11.1.2, 11.1.3 for SAC review.*
Version 1.3 – July 26, 2006	*Made modifications as a result of the SAC and legal commentary to sections 1,2,5,9 and 11.*
Version 1.3 – August 15, 2006	*Minor adjustments to new policies introduced in v1.2 and v1.3, fixed spelling errors.*
Version 1.3 – September 14, 2006	*Version 1.3 approved for publication.*
Version 1.4 – August 8, 2007	*Minor wording changes throughout. Major wording changes to 9.5.*
Version 1.5 – January 8, 2008	*Minor wording changes to 9.5. Added policy 9.5.2.*
Version 1.6 – April 4, 2008	*Minor wording changes to 9.5.2.*

14. TERMS AND DEFINITIONS

See Appendix J

http://www.intranet.state.tn.us/finance/oir/qa/stds/glossary/index.htm

15. APPENDICES

- Appendix A Security Policy Development Process
- Appendix B Security Policy Development Process Flow Diagram
- Appendix C Security Policy Exception Process
- Appendix D Security Policy Exception Process Flow Diagram
- Appendix E Security Policy Action Request
- Appendix F NIST SP-800-47 *(Temporary Substitution for "Security Requirements for Enterprise Interconnectivity)*
- Appendix G State of Tennessee Acceptable Use Policy
- Appendix H State of Tennessee Approved Login Banner
- Appendix I Security Policy Compliance Matrix
- Appendix J Glossary
- Appendix K Information Security Incident Response Plan
- Appendix L Third Party Access Agreement
- Appendix M IT Control Framework
- Appendix N Security Policy Exception Request Form